Wi-Fi Usage in Voting (with vendor complicity)

Jeremy Epstein

Sep 29 2005

Taxonomy

Wholesale at the precinct level.

Applicability

Voting phases: Any system using Wi-Fi (typically but not exclusively DREs), whether or not the Wi-Fi is intentionally used. There is at least one model of DRE that uses Wi-Fi (the AVS WinVote); there may be others. Additionally, since many DREs are based on off-the-shelf laptop computers which have built-in Wi-Fi[1], there may be products that have Wi-Fi capabilities that are not advertised, and perhaps not even known by the DRE vendor.

Method

Many voting machines use Wi-Fi (wireless networking, typically following the IEEE 802.11b or 802.11g standards) for communication among machines in a precinct. In some cases, they are used for opening and closing the polls, while in other cases they might be used during the day.

This example assumes that the perpetrator has the ability to modify the software used in the voting machine, either by being part of the development effort at the vendor, or by modifying the software during programming in the local jurisdiction. Other Wi-Fi examples submitted separately do not assume the ability to modify software.

The perpetrator causes the voting machine software to be enabled at an opportune time, and to accept commands once a “secret” enablement command has been provided[2]. This can be hidden from detection (see *Likelihood of Detection*, below). Once the Wi-Fi link is enabled, the attacker can retrieve vote totals and/or ballot programming, modify the settings, and download new totals and/or programming. For example, the programming

---

[1] Nearly any laptop using the popular Pentium M chipset will have Wi-Fi.

[2] The concept of using a secret enablement command is widely used by attackers on the internet, not specifically for voting machines, but for other forms of attacks involving “back doors”.

could be modified to add every fourth vote for Jane Jones to the total for Sam Smith instead, while displaying the correct values on the screen.[3]

Another related alternative which could be used by the perpetrator is to cause the Wi-Fi communication to use a weak or predetermined encryption key. This is effectively impossible to detect without a careful cryptographic analysis, which is well beyond the scope of voting machine testing.

Resource Requirements

There are two roles who must be complicit in this example: the insider who introduces the flaw, and the person who exploit it on election day. These could be the same person or different people.

For the first role, the perpetrator must have the ability to modify the software used in the voting system, either as a member of the vendor's development team or during the local programming.

Stealing a local election would be fairly easy this way, since a person in the second role can go from precinct to precinct making the appropriate "zaps" to voting machines. On a broader base (e.g., a statewide election) would require more people to divide up the work, since it can only be done as fast as each machine can be remotely accessed.

Potential Gain

- Ability to shut down as many precincts as can be visited on election day by the perpetrator and his/her co-conspirators (known as a "denial of service" attack).
- Ability to make arbitrary modifications to the voting totals at as many precincts as can be visited on election day by the perpetrator and his/ her co-conspirators.
- Ability to make arbitrary modifications to the ballot setup at as many precincts as can be visited on election day by the perpetrator and his/ her co-conspirators.

Likelihood of Detection

The likelihood of detection can be made arbitrarily small. For example, software could enable the Wi-Fi device for a few seconds every ten minutes while the polls are open; if an enablement command is received during that window, the device is left enabled, and otherwise disabled. This would be almost impossible to detect as part of Logic & Accuracy tests, since continuous scanning for an open Wi-Fi link is unlikely. Even if the brief on period is detected during testing, without knowing the enablement command to keep the connection open permanently, it would likely be dismissed as a testing error.

[3] Such actions have happened by accident in voting system demonstrations. Whether they have happened in real elections is unproven, but is a matter of debate.

An attacker need not be inside the polling place to launch attacks. A Pringles® potato chip can is a highly effective receiver for Wi-Fi traffic[4], allowing access from a substantial distance (e.g., a car driving within several hundred yards of the precinct). Further, it would only take a few seconds to modify the programming once the Wi-Fi link is enabled, thus allowing the attacker to perform the reprogramming without even parking his/her car.

Encrypting the Wi-Fi traffic (the most commonly described protection for Wi-Fi) is not a countermeasure to this type of attack.

Countermeasures

Preventative Measures

Source code review will make it harder to hide code to enable the Wi-Fi enabling. However, source code review is only moderately effective even when security flaws are accidental, and is reasonably ineffective against deliberately hidden flaws.

Requiring hardware for voting machines that does not have any Wi-Fi features completely prevents this type of attack. As Wi-Fi is increasingly built into laptop computers (the basis for most DREs), this is increasingly infeasible.

Having all voting machines inside a Faraday cage, such as is used for processing classified information (where it is known as a SCIF). This would require that the attacker be inside the same facility, making a remote attack impossible (but local attacks would still be undetectable). Equipping every precinct as a Faraday cage is impractical, and putting each voting machine inside a Faraday cage is equivalent to disabling the Wi-Fi, thus eliminating any benefit it might have.

Detection Measures

Detection is difficult if the modifications made in vote totals are relatively small, but a 5% change in vote totals could easily be made without detection.

Voting systems that provide a paper backup (e.g,. optical scan or DRE with VVPAT) can be recounted; a hand recount would detect any tampering.

If the attacker adds ballots rather than modifying those that have already been voted (or are yet to be voted), then a reconciliation of the number of votes vs. the number of voters will detect the attack.

Citations

---

[4] A report in 2001 gave the cost of building a Pringles® antenna at under $7 each, or less if built in bulk. See http://www.oreillynet.com/cs/weblog/view/wlg/448 for details.

None.

Retrospective

This is a variation on stuffing the ballot box. It does not require physical access to the voting machine, and operates by replacing ballots rather than adding new ones.